ANTHONY L. RAFEL, OSB 066472
arafel@rafellawgroup.com
Rafel Law Group PLLC
1100 SW 6th Ave., Ste. 1600
Portland, OR 97204
Tel: 503-808-9960; Fax: 503-243-2687

TINA WOLFSON (*pro hac vice* application to be filed)
twolfson@ahdootwolfson.com
ROBERT AHDOOT (*pro hac vice* application to be filed)
rahdoot@ahdootwolfson.com
THEODORE W. MAYA (*pro hac vice* application to be filed)
tmaya@ahdootwolfson.com
AHDOOT & WOLFSON, P.C.
1016 Palm Ave.
West Hollywood, California 90069
Tel: 310-474-9111; Fax: 310-474-8585

Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

PORTLAND DIVISION

DARIN PURCELL, on his own behalf and on behalf of all others similarly situated, Plaintiffs, v. **PREMERA BLUE CROSS**, a Washington nonprofit corporation; and DOES 1-50, Defendants.	Case No. **CLASS ACTION COMPLAINT** Breach of Contract Action (28 U.S.C. § 1332) JURY TRIAL DEMANDED

Plaintiff Darin Purcell ("Plaintiff"), by and through his counsel, brings this Class Action Complaint against Defendant Premera Blue Cross on behalf of himself and all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsel's investigations, and upon information and belief as to all other matters, as follows:

PARTIES

1. Defendant Premera Blue Cross ("Defendant") is a Washington nonprofit corporation with headquarters located at 7001 220th Street SW, Mountlake Terrace, Washington, 98043. Defendant conducts business throughout this District and the United States.

2. Plaintiff Darin Purcell ("Plaintiff") is an individual and currently a resident of Milwaukie, Oregon, who is insured through Defendant.

3. Plaintiff is unaware of the true names and capacities of the defendants sued as DOES 1-50, and therefore sues these defendants by fictitious names. Plaintiff will seek leave to amend this Complaint when and if the true identities of these DOE defendants are discovered. Plaintiff is informed and believes and thereon alleges that each of the Defendants designated as a DOE is responsible in some manner for the acts and occurrences alleged herein, whether such acts or occurrences were committed intentionally, negligently, recklessly or otherwise, and that each said DOE defendant thereby proximately caused injuries and damages to Plaintiff as herein alleged, and is thus liable for the damages suffered by Plaintiff.

JURISDICTION AND VENUE

4. This Court has original jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d), because this is a class action in which (i) the proposed class consists of more than 100 members; (ii) at least some members of the proposed class are citizens of a state different from any defendant; and (iii) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

5. This Court has personal jurisdiction over Defendant because Defendant is authorized to, and does, business in the State of Oregon, providing health insurance to citizens of this State such as Plaintiff.

6. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a) because Defendant resides in this District and a substantial part of the events that give rise to the claims herein occurred in this District.

FACTUAL BACKGROUND

7. In what appears to be the largest data breach reported to date involving patient medical information, health insurer Premera Blue Cross ("Defendant"), through its deficient cybersecurity, exposed medical data and financial information of 11 million of its insureds and customers.

8. As a result of Defendant's deficient security, hackers appear to have gained access to claims data, including clinical information, along with banking account numbers, Social Security numbers, birth dates, a variety of personally identifiable information ("PII"), and other data in an attack that began at least as early as May 2014 (the "Data Breach").

9. By May 5, 2014, hackers infiltrated Defendant's Information Technology ("IT") system and, for months thereafter, had access to as many as 11 million records of current and former insureds and employees, as well as Blue Cross Blue Shield customers who received medical treatment in Washington or Alaska. The hackers were able to access these individuals' names, dates of birth, email addresses, addresses, telephone numbers, Social Security numbers, member identification numbers, bank account information, claims information including clinical data, and other information.

10. Defendant has stated that the Data Breach affected current and former customers of Premera Blue Cross, Premera Blue Cross Blue Shield of Alaska, and affiliates, including Vivacity and Connexion Insurance Solutions, Inc. Several days after the breach, LifeWise Health Plan of Oregon announced that 60,000 of its members were compromised by the Data Breach.

11. Defendant further acknowledged that the breach affected members of any Blue Cross Blue Shield plan who had received medical treatment in Washington or Alaska, and that "[i]ndividuals who do business with us and provided us with their email address, personal bank

account number or social security number are also affected." <http://www.premeraupdate.com/> (statement of Jeffrey Roe) (last visited Mar. 30, 2015).

12. On information and belief, Defendant failed properly to segregate medical information from other PII and financial information.

13. The federal government explicitly warned Defendant that its cyber security systems were vulnerable before the Data Breach occurred. On April 18, 2014, the Office of Personnel Management delivered the results of an audit it performed on Premera's IT systems. The audit identified ten areas in which Defendant's systems were inadequate and vulnerable to attack. *See* Mike Baker, *Feds Warned Premera About Security Flaws Before Breach*, SEATTLE TIMES, Mar. 18, 2015, *available at* <http://www.seattletimes.com/business/local-business/feds-warned-premera-about-security-flaws-before-breach/> (last visited Mar. 30, 2015).

14. The audit found that Premera was not implementing critical security patches and other software updates and warned: "Failure to promptly install important updates increases the risk that vulnerabilities will not be remediated and sensitive data could be breached." U.S. Office of Personnel Management, Office of the Inspector General, *Final Audit Report* at 7 (Nov. 8, 2014), *available at* <https://s3.amazonaws.com/s3.documentcloud.org/documents/1688453/opm-audit.pdf> (last visited Mar. 30, 2015).

15. Instead of responding to the federal audit, implementing the Inspector General's recommendations, and immediately strengthening its IT security, Defendant allowed itself to remain vulnerable and, predictably, allowed the Data Breach to occur months after the federal audit was completed.

16. The hackers appear to have accessed the PII and medical information in unencrypted form, or to have obtained a key allowing the information to be unencrypted. *See, e.g.*, Joseph Goedert, *Premera Breach Highlights Need for Encryption*, HealthData Management, Mar. 19, 2015, *available at* <http://www.healthdatamanagement.com/news/Decision-to-Forgo-Encryption-Costing-Health-Organizations-Dearly-50014-1.html> (last visited Mar. 30, 2015).

17. Plaintiff received vaguely worded notices on March 17, 2015, that his PII and medical information, as well as that of his entire immediate family, members of which also are

insured through Defendant, has been compromised in the Data Breach. Copies of these notices are attached hereto as **Exhibit A**.

18. Medical records are highly valuable on underground criminal exchanges where stolen data is sold because the information can be used to engage in insurance fraud, and because the PII involved can be used to engage in a variety of other crimes, including financial identity theft, for instance by using one's social security number to open new accounts in a victim's name.

19. Defendant did not disclose the Data Breach until March 17, 2015, despite having known about it since at least January 29, 2015, according to its own account of events.

20. Defendant has not yet fully and accurately informed its insureds regarding the scope of the Data Breach or the risks of identity theft. It is not clear how many insureds Defendant has notified to date, but Defendant itself estimates that it will not complete the notification process until April 20, 2015 — approximately three months after the Data Breach.

21. It is critical that companies affected by data breaches provide timely, accurate, and complete information to those whose information has been compromised so they can take necessary precautions to protect themselves and their families from further harm. Accordingly, the Health Insurance Portability and Accountability Act ("HIPAA") requires that Defendant provide notice without unreasonable delay and no later than 60 days after discovery of a breach. *See* 45 C.F.R. § 164.404. Washington state law similarly requires Defendant to provide notice in the most expedient time possible. *See* Wash. Rev. Code § 19.255.010. Oregon law also requires notice in the most expedient time possible and without unreasonable delay. Or. Rev. Stat. §§ 646A.600 *et seq.*

22. As a result of the Data Breach, Plaintiff and members of the Class will have to take a variety of steps to monitor for and safeguard against identity theft and are at a much greater risk of suffering such identity theft, which may well include fraudulent medical care in the victims' names, charges for such medical care, and/or adulteration of the victims' true medical records in possibly dangerous ways. In addition, these victims of the Data Breach are at a heightened risk of potentially devastating financial identity theft. As the Bureau of Justice

reports, identity theft causes its victims out-of-pocket monetary losses and costs the nation's economy billions of dollars every year. *See* U.S. Dept. of Justice, Bureau of Justice Statistics, *Victims of Identity Theft, 2012* (Dec. 2013), *available at* <http://www.bjs.gov/content/pub/pdf/vit12.pdf> (last visited Mar. 30, 2015).

23. Loss of social security numbers, such as those disclosed through the Data Breach that Defendant failed to prevent, can be especially devastating, as thieves can use such information, in combination with the other PII stolen, to open new accounts in victims' names without their knowledge, and even to obtain fraudulent encumbrances on such victims' property.

24. Defendant breached its duty (a) to protect and safeguard its insureds' PII and medical information, and (b) to notify those affected in a timely and complete manner. Plaintiff brings this action on behalf of himself and similarly situated insureds whose PII and medical information was compromised in the Data Breach, for compensation for the injuries they have suffered and for injunctive relief to ensure that Defendant takes proper security precautions in the future and gives prompt and full information to all affected people concerning their exposure through the Data Breach.

CLASS ACTION ALLEGATIONS

25. Plaintiff brings this action on behalf of a nationwide class preliminarily defined as:

> All current or former insureds of Premera Blue Cross residing in the United States whose personal and/or medical information was compromised in the data breach disclosed by Premera Blue Cross on or about March 17, 2015.

(The "Nationwide Class.") Excluded from the Nationwide Class are Defendant; any agent, affiliate, parent, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any officer or director of Defendant; any successor or assign of Defendant; and any Judge to whom this case is assigned as well as his or her staff and immediate family.

26. Plaintiff also brings this action on behalf of an Oregon State Class, preliminarily defined as:

> All current or former insureds of Premera Blue Cross residing in the State of Oregon whose personal and/or medical information was compromised in the data breach disclosed by Premera Blue Cross on or about March 17, 2015.

(The "Oregon Class.") Excluded from the Oregon Class are Defendant; any agent, affiliate, parent, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any officer or director of Defendant; any successor or assign of Defendant; and any Judge to whom this case is assigned as well as his or her staff and immediate family.

27. Plaintiff satisfies the numerosity, commonality, typicality, and adequacy prerequisites for suing as a representative party under Rule 23.

28. **Numerosity.** The proposed Nationwide Class consists of more than 11 million members—far too many to join in a single action, and although the Oregon Class is smaller, on information and belief the Oregon Class consists of thousands of members, at a minimum, and also satisfies the numerosity requirement.

29. **Ascertainability.** Class members are readily identifiable from information in Defendant's possession, custody, or control.

30. **Typicality.** Plaintiff's claims are typical of class members' claims as each arises from the same Data Breach, the same alleged negligence of and/or statutory violations by Defendant, and the same unreasonable manner of notifying Defendant's insureds regarding the Data Breach.

31. **Adequacy.** Plaintiff will fairly and adequately protect the interests of the all proposed classes. His interests do not conflict with class members' interests and he has retained counsel experienced in complex class action litigation and medical data privacy to vigorously prosecute this action on behalf of both classes.

32. **Commonality.** Plaintiff's and class members' claims raise predominantly common factual and legal questions that can be answered for all class members through a single class-wide proceeding. For example, to resolve any class member's claims, it will be necessary to answer the following questions. The answer to each of these questions will necessarily be the same for each class member.

a. Whether Defendant unlawfully used, maintained, lost or disclosed Class members' personal, financial, and/or information;

b. Whether Defendant unreasonably delayed in notifying affected individuals of the Data Breach and whether the belated notice was adequate;

c. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

d. Whether Defendant's conduct was negligent;

e. Whether Defendant's conduct in connection with the Data Breach and notification thereof violated HIPAA;

f. Whether Defendant's conduct in connection with the Data Breach and notification thereof violated Washington State law;

g. Whether Defendant's conduct in connection with the Data Breach and notification thereof violated Oregon State Law;

h. Whether Defendant's conduct in connection with the Data Breach and notification thereof breached the terms of any implied and/or express contracts between it and Class members;

i. Whether Plaintiffs and the Class are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

33. In addition to satisfying the prerequisites of Rule 23(a), Plaintiffs satisfy the requirements for maintaining a class action under Rule 23(b). Common questions of law and fact predominate over any questions affecting only individual members and a class action is superior to individual litigation. The damages available to individual plaintiffs are insufficient to make litigation addressing Defendants' medical privacy practices economically feasible in the absence of the class action procedure.

34. In the alternative, the class certification is appropriate because Defendants have acted or refused to act on grounds generally applicable to the class, thereby making final injunctive relief appropriate with respect to the members of the class as a whole.

FIRST CAUSE OF ACTION

Negligence

(On Behalf of Plaintiff and All Classes)

35. Plaintiff incorporates by reference all other paragraphs alleged herein.

36. Defendant required Plaintiff and class members to submit non-public PII and medical information in order to acquire coverage under a health insurance policy and/or receive medical treatment.

37. Defendant collected and stored this PII and medical information.

38. Defendant assumed a duty of care to use reasonable means to secure and safeguard this PII and medical information, to prevent disclosure of the information, to guard the information from theft, and to detect any attempted or actual breach of its IT systems.

39. Defendant breached its duty of care by failing to secure and safeguard the PII and medical information of Plaintiff and other members of the classes. Defendant negligently maintained systems that it knew were vulnerable to a security breach, despite being made aware of these vulnerabilities any number of ways, including through the federal government's audit of those very systems. Defendant negligently stored PII and medical information in an unencrypted form on a single, highly vulnerable database.

40. Defendant continues to breach this duty of care by failing to share crucial, complete information with Plaintiff and other members of the classes in a timely manner.

41. Plaintiff and the other members of the classes have suffered harm as a result of Defendant's negligence. These victims' loss of control over the PII and medical information exposed subjects each of them to a greatly enhanced risk of identity theft, medical identity theft, credit and bank fraud, Social Security fraud, tax fraud, and myriad other types of fraud and theft. Plaintiff and other members of the proposed classes suffered and continue to suffer further harm by virtue of Defendant's failure to give timely and complete notice to them concerning the Data Breach and the risks they face.

42. Plaintiff and other members of the classes are entitled to injunctive relief as well as actual and punitive damages, including under Or. Rev. Stat. §§ 31.730 and 646.638.

SECOND CAUSE OF ACTION

Negligence *per se*

(On Behalf of Plaintiff and All Classes)

43. Plaintiff incorporates by reference all other paragraphs alleged herein.

44. Under HIPAA, Defendant had a duty to secure and safeguard the personal information of its customers. Defendant acknowledged this duty to its customers in its Notice of Privacy Practices, and warranted that it would comport with its duties under HIPAA.

45. Defendant violated HIPAA by failing to secure and safeguard the PII and medical information belonging to Plaintiff and other members of the classes; by failing to implement protections against "reasonably anticipated threats," 45 C.F.R. § 164.306; by failing to encrypt the PII and medical information, *id*. § 164.312; and by failing to notify Plaintiff and other members of the classes in accordance with the requirements set forth at 45 CFR § 164.404.

46. Defendant further violated notification requirements under state law, including Wash. Rev. Code § 19.255.010 and Or. Rev. Stat. § 646A.604, and state law that required Defendant properly to safeguard Defendant's PII and medical information, including Wash. Rev. Code § 19.255.020 and Or. Rev. Stat. § 646A.622. These actions constitute negligence *per se*.

47. Plaintiff and the other members of the classes have suffered harm as a result of Defendant's negligence *per se*. These victims' loss of control over the PII and medical information exposed subjects each of them to a greatly enhanced risk of identity theft, medical identity theft, credit and bank fraud, Social Security fraud, tax fraud, and myriad other types of fraud and theft. Plaintiff and other members of the proposed classes suffered and continue to suffer further harm by virtue of Defendant's failure to give timely and complete notice to them concerning the Data Breach and the risks they face.

48. Plaintiff and other members of the classes are entitled to injunctive relief as well as actual and punitive damages, including under Or. Rev. Stat. §§ 31.730 and 646.638.

THIRD CAUSE OF ACTION

Bailment

(On Behalf of Plaintiff and All Classes)

49. Plaintiff incorporates by reference all other paragraphs alleged herein.

50. Plaintiff and other members of the proposed classes delivered and entrusted their PII and medical information to Defendant for the sole purpose of receiving health insurance services and/or medical treatment from Defendant.

51. By delivering their PII and medical information to Defendant, Plaintiff and other members of the proposed classes intended and understood that Defendant would safeguard adequately their PII and medical information against hacking and/or disclosure to unauthorized persons.

52. By accepting possession of the PII and medical information belonging to Plaintiff and other members of the proposed classes, Defendant understood that Plaintiff and other members of the proposed classes expected Defendant to safeguard adequately their PII and medical information.

53. Defendant accepted possession of the PII and medical information belonging to Plaintiff and other members of the proposed classes for the purpose of providing health insurance and/or medical treatment to them. Thus, a bailment (or deposit) was established for the mutual benefit of the parties.

54. During the time of bailment, Defendant owed Plaintiff and other members of the proposed classes a duty to safeguard this information properly and maintain reasonable security procedures and practices to protect such information.

55. Defendant breached this duty.

56. Plaintiff and the other members of the classes have suffered harm as a result of Defendant's breach of its bailment and of its duty of care. These victims' loss of control over the PII and medical information exposed subjects each of them to a greatly enhanced risk of identity theft, medical identity theft, credit and bank fraud, Social Security fraud, tax fraud, and myriad other types of fraud and theft. Plaintiff and other members of the proposed classes suffered and

continue to suffer further harm by virtue of Defendant's failure to give timely and complete notice to them concerning the Data Breach and the risks they face.

57. Plaintiff and other members of the classes are entitled to injunctive relief as well as actual and punitive damages, including under Or. Rev. Stat. §§ 31.730 and 646.638.

FOURTH CAUSE OF ACTION

Breach of Contract

(On Behalf of Plaintiff and all Classes)

58. Plaintiff incorporates by reference all other paragraphs alleged herein.

59. Defendant entered into written (or, in the alternative implied) contracts with Plaintiffs and the Class in which it agreed to provide health insurance in exchange for periodic payments of premiums.

60. Under the terms of this contractual agreement, Defendant was obliged to maintain the security of its insureds' PII and medical information, and to comply with HIPAA.

61. Defendant breached its contractual obligations by failing to secure and safeguard the PII and medical information of Plaintiff and other members of the classes. Defendant negligently maintained systems that it knew were vulnerable to a security breach, despite being made aware of these vulnerabilities any number of ways, including through the federal government's audit of those very systems. Defendant negligently stored PII and medical information in an unencrypted form on a single, highly vulnerable database.

62. Defendant continues to breach its contractual obligations by failing to share crucial, complete information with Plaintiff and other members of the classes in a timely manner.

63. Plaintiff and the other members of the classes have suffered harm as a result of Defendant's breach of contract. These victims' loss of control over the PII and medical information exposed subjects each of them to a greatly enhanced risk of identity theft, medical identity theft, credit and bank fraud, Social Security fraud, tax fraud, and myriad other types of fraud and theft. Plaintiff and other members of the proposed classes suffered and continue to suffer further harm by virtue of Defendant's failure to give timely and complete notice to them concerning the Data Breach and the risks they face.

FIFTH CAUSE OF ACTION

Breach of Fiduciary Duty

(On Behalf of Plaintiff and all Classes)

64. Plaintiff incorporates by reference all other paragraphs alleged herein.

65. As the health insurance provider to Plaintiff and other members of the proposed classes, Defendant owed such persons a fiduciary duty, which included the duty to safeguard this information properly and maintain reasonable security procedures and practices to protect such information, and to keep Plaintiff and other members of the proposed classes fully informed in a timely manner regarding the Data Breach.

66. Defendant breached its fiduciary duties by failing to secure and safeguard the PII and medical information of Plaintiff and other members of the classes. Defendant negligently maintained systems that it knew were vulnerable to a security breach, despite being made aware of these vulnerabilities any number of ways, including through the federal government's audit of those very systems. Defendant negligently stored PII and medical information in an unencrypted form on a single, highly vulnerable database.

67. Defendant continues to breach its fiduciary duties by failing to share crucial, complete information with Plaintiff and other members of the classes in a timely manner.

68. Plaintiff and the other members of the classes have suffered harm as a result of Defendant's breach of fiduciary duty. These victims' loss of control over the PII and medical information exposed subjects each of them to a greatly enhanced risk of identity theft, medical identity theft, credit and bank fraud, Social Security fraud, tax fraud, and myriad other types of fraud and theft. Plaintiff and other members of the proposed classes suffered and continue to suffer further harm by virtue of Defendant's failure to give timely and complete notice to them concerning the Data Breach and the risks they face.

69. Plaintiff and other members of the classes are entitled to injunctive relief as well as actual and punitive damages, including under Or. Rev. Stat. §§ 31.730 and 646.638.

SIXTH CAUSE OF ACTION

Violation of Washington's Data Disclosure Law, Wash. Rev. Code § 19.255.010-020

(On Behalf of Plaintiff and the Nationwide Class)

70. Plaintiff incorporates by reference all other paragraphs alleged herein.

71. Under Wash. Rev. Code § 19.255.010, Defendant is required to disclose "any breach of the security of the data immediately following discovery" of a data breach, "in the most expedient time possible and without unreasonable delay."

72. Under Wash. Rev. Code § 19.255.020, Defendant is required to exercise "reasonable care to guard against unauthorized access to" the PII and medical information disclosed in the Data Breach.

73. Defendant failed to disclose the Data Breach in the most expedient time possible, and failed to exercise reasonable care to prevent the Data Breach.

74. Plaintiff seeks damages as permitted by law, as well as injunctive relief. As of this filing, Defendant has not provided notice to victims of the Data Breach consistent with the requirements of Washington law, and it should be compelled to do so without delay.

SEVENTH CAUSE OF ACTION

Violation of the Washington Consumer Protection Act, Wash. Rev. Code § 19.86 *et seq.*

(On Behalf of Plaintiff and the Nationwide Class)

75. Plaintiff incorporates by reference all other paragraphs alleged herein.

76. Defendant is a "person" within the meaning of the Washington Consumer Protection Act, Wash. Rev. Code § 19.86.010(1), and conducts "trade" and "commerce" within the meaning of § 19.86.010(2).

77. Plaintiff and other members of the Nationwide Class are "persons" within the meaning of § 19.86.010(1).

78. Defendant's failure to safeguard the PII and medical information disclosed in the Data Breach constitutes an unfair act that offends public policy, including as set forth in HIPAA and the state laws cited *supra*.

79. Defendant's failure to promptly and fully notify Plaintiff and other Class

members regarding the Data Breach is unfair because these acts or practices offend public policy, including as set forth in HIPAA and the state laws cited *supra*.

80. Defendant's failure to safeguard the PII and medical information disclosed in the Data Breach, and its failure to provide timely and complete notice of that Data Breach to the victims, causes substantial injury to Plaintiff and other Class members, is not outweighed by any countervailing benefits to consumers or competitors, and is not reasonably avoidable by consumers.

81. Defendant's failure to safeguard the PII and medical information disclosed in the Data Breach, and its failure to provide timely and complete notice of that Data Breach to the victims, is unfair because these acts and practices are immoral, unethical, oppressive and/or unscrupulous.

82. Defendant's unfair acts or practices occurred in its trade or business and have and are capable of injuring a substantial portion of the public. Defendant's general course of conduct as alleged herein is injurious to the public interest, and the acts complained of herein are ongoing and/or have a substantial likelihood of being repeated.

83. As a direct and proximate result of Defendant's unfair acts or practices, Plaintiff and other Class members suffered injury in fact.

84. Plaintiff and other Class members are entitled to an order enjoining the conduct complained of herein and ordering Defendant to take remedial measures to prevent similar data breaches from occurring in the future; actual damages; treble damages pursuant to Wash. Rev. Code § 19.86.090; costs of suit, including reasonable attorney fees; and such further relief as the Court may deem proper.

EIGHTH CAUSE OF ACTION

Violation of Oregon's Unlawful Trade Practices Act, Or. Rev. Stat. §§ 646.608 *et seq.*

(On Behalf of Plaintiff and the Oregon Class)

85. Plaintiff incorporates by reference all other paragraphs alleged herein.

86. The Data Breach alleged above constituted a "breach of security" within the meaning of Or. Rev. Stat. § 646.602(l)(a).

87. The PII and medical information disclosed in the Data Breach constituted "personal information" within the meaning of Or. Rev. Stat. § 646.602(11).

88. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach.

89. Defendant unreasonably delayed informing Plaintiff and other Class members about the Data Breach after Defendant knew the Data Breach occurred, without reasonable excuse.

90. Defendant's failure to implement reasonable security measures, to promptly notify Plaintiff and other Class members, and otherwise to comply with Or. Rev. Stat. § 646A.600 *et seq.* is an unlawful, unfair, and deceptive practice under § 646.608(1)(u).

91. Defendant's failure to safeguard the PII and medical information disclosed in the Data Breach, and its failure to provide timely and complete notice of that Data Breach to the victims, constitutes an unfair act because these acts and practices offend public policy as it has been established by statutes, regulations, the common law or otherwise, including the public policy established by Or. Rev. Stat. § 646A.600 *et seq*.

92. Defendant's failure to safeguard the PII and medical information disclosed in the Data Breach, and its failure to provide timely and complete notice of that Data Breach to the victims, causes substantial injury to Plaintiff and other Class members, is not outweighed by any countervailing benefits to consumers or competitors, and is not reasonably avoidable by consumers.

93. Defendant's failure to safeguard the PII and medical information disclosed in the Data Breach, and its failure to provide timely and complete notice of that Data Breach to the victims, is unfair because these acts and practices are immoral, unethical, oppressive and/or unscrupulous.

94. Defendant's unfair acts or practices occurred in its trade or business and have and are capable of injuring a substantial portion of the public. Defendant's general course of conduct as alleged herein is injurious to the public interest, and the acts complained of herein are ongoing

and/or have a substantial likelihood of being repeated.

95. As a direct and proximate result of Defendant's unfair acts or practices, Plaintiff and other Class members suffered injury in fact.

96. Plaintiff, individually and on behalf of the Oregon Class, seeks all remedies available under Or. Rev. Stat. § 646.605 *et seq*., including equitable relief, actual damages, statutory damages, and punitive damages, including under Or. Rev. Stat. § 646.638.

97. Plaintiff, individually and on behalf of the Oregon Class, also seeks reasonable attorneys' fees and costs under Or. Rev. Stat. § 646.638(3).

NINTH CAUSE OF ACTION

Unjust Enrichment

(On Behalf of Plaintiff and All Classes)

98. Plaintiff incorporates by reference all other paragraphs alleged herein.

99. If the Court finds Plaintiff's and other Class members' contracts with Defendant for protection of their PII and medical information invalid, non-existent, or otherwise unenforceable, Plaintiff and other Class members may be left without any adequate remedy at law.

100. Plaintiff and other Class members conferred a monetary benefit on Defendant in the form of fees paid for healthcare insurance. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and other Class members.

101. The fees that Plaintiff and other Class members paid to Defendant were supposed to be used by Defendant, in part, to pay for the costs of reasonable data management and security, including encryption of PII and medical information.

102. Under principles of equity and good conscience, Defendant should not be permitted to retain the paid by Plaintiff and other Class members, because Defendant failed to implement reasonable cyber security measures that Plaintiff and other Class members paid for and that are mandated by HIPAA, by the state laws cited above, and by industry standards.

103. As a result of Defendant's conduct, Plaintiff and other Class members suffered damages in the amount of the difference between the price they paid for Defendant's insurance

as promised and the actual diminished value of what they received.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff makes the following prayer for relief, on behalf of himself and the proposed classes:

a. An order certifying the proposed classes pursuant to Federal Rule of Civil Procedure 23 and appointing Plaintiff and his counsel to represent the classes;

b. An order awarding Plaintiff and other Class members monetary relief, including actual, statutory, and punitive damages;

c. Equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and other Class members' PII and medical information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and other Class members;

d. Equitable relief compelling Defendant to utilize appropriate methods and policies with respect to its data collection, storage, and safety practices and to disclose with specificity to Class members the type of data compromised in the Data Breach, and other information required under the laws cited herein;

e. Equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

f. An award of costs of suit and attorneys' fees, as allowable by law;

g. An award of pre-judgment and post-judgment interest, as provided by law;

h. Leave to amend this Complaint to conform to the evidence produced at trial; and

i. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all claims so triable.

DATED: April 7, 2015

Respectfully submitted,

By: */s Anthony L. Rafel*
ANTHONY L. RAFEL, OSB 066472
arafel@rafellawgroup.com
Rafel Law Group PLLC
1100 SW 6th Ave., Ste. 1600
Portland, OR 97204
Tel: 503-808-9960; Fax: 503-243-2687

AHDOOT & WOLFSON, PC
Tina Wolfson (*pro hac vice* application to be filed)
Robert Ahdoot (*pro hac vice* application to be filed)
Theodore W. Maya (*pro hac vice* application to be filed)
1016 Palm Ave.
West Hollywood, California 90069
Telephone: 310-474-9111
Facsimile: 310-474-8585